IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION

Invicta Networks, Inc.

Plaintiff,

v.

Forcepoint LLC

Defendant.

Civil Action No. 6:20-cv-00173

The Honorable ________________________

COMPLAINT FOR PATENT INFRINGEMENT

JURY TRIAL DEMANDED

COMPLAINT FOR PATENT INFRINGEMENT AND DEMAND FOR JURY TRIAL

TO THE HONORABLE JUDGE OF SAID COURT:

Plaintiff Invicta Networks, Inc. ("Invicta"), files this Complaint for Patent Infringement and Damages against Defendant Forcepoint LLC ("Forcepoint"), and would respectfully show the Court as follows:

PARTIES

1. Plaintiff Invicta is a Delaware Corporation with its principal place of business located at 10217 Cedar Pond Drive, Vienna, VA 22182.

2. On information and belief, Defendant Forcepoint is a Delaware limited liability company, and a wholly-owned subsidiary of Raytheon Company. Forcepoint's headquarters and principal place of business is located at 10900-A Stonelake Blvd., Quarry Oaks 1, Suite 350, Austin, TX 78759. Raytheon is a Delaware Corporation.

JURISDICTION AND VENUE

3. This is a civil action for patent infringement arising under the Patent Laws of the United States as set forth in 35 U.S.C. §§ 271, *et seq*.

4. This Court has federal subject matter jurisdiction over this action pursuant to 28 U.S.C. §§ 1331 and 1338(a) and pendant jurisdiction over the other claims for relief asserted herein.

5. This Court has personal jurisdiction over Defendant because Defendant is a resident of Texas, with its principal place of business and headquarters located at 10900-A Stonelake Blvd., Quarry Oaks 1, Suite 350, Austin, TX 78759. On information and belief, Defendant has approximately 500 employees in its Austin, Texas headquarters, with a wide range of jobs including corporate administration, sales and marketing, engineering, research and development, and customer support. For example:

(i) <https://www.statesman.com/news/20190228/digital-dilemma-is-austin-cybersecurity-hub-depends-who-you-ask>;

(ii) <https://www.statesman.com/news/20190305/austin-cybersecurity-firm-forcepoint-steps-into-behavioral-science-research>; and

(iii) <https://www.google.com/search?q=forcepoint+jobs+austin+texas&ibp=htl;jobs&sa=X&ved=2ahUKEwjzsuau-uLnAhXQZd8KHWAbCKEQiYsCKAB6BAgKEAM#htivrt=jobs&htidocid=pcRQz-3EexTPgHsOAAAAAA%3D%3D&fpstate=tldetail>

By virtue of filing this complaint, Plaintiff voluntarily consents to this Court's jurisdiction.

6. Venue is proper in this Court under 28 U.S.C. §§ 1391(b) and (c) and 28 U.S.C. § 1400(b) because Defendant is domiciled in Texas, within this district, with its headquarters and principal place of business located at 10900-A Stonelake Blvd., Quarry Oaks 1, Suite 350, Austin, TX 78759. In addition, venue is proper in this Court based on the information and belief that

Defendant has committed or induced acts of infringement, and/or advertise, market, support, sell, and/or offer to sell products, including infringing products, in this judicial district.

THE PATENT-IN-SUIT

7. On March 7, 2006, United States Patent No. 7,010,698 ("the '698 patent"), entitled "Systems and Methods for Creating a Code Inspection System" was duly and legally issued by the United States Patent and Trademark Office ("USPTO") to Victor I. Sheymov, with Invicta Networks, Inc. ("Invicta") as assignee. A copy of the '698 patent is attached hereto as **Exhibit A**.

8. Plaintiff Invicta Networks, Inc., is the owner of the entire right, title, and interest in and to the '698 patent, which is presumed valid under 35 U.S.C. § 282.

United States Patent No. 7,010,698

9. The '698 patent claims a number of embodiments for code inspection systems, methods for creating and maintaining decoy systems, and information storage media.

a. Claim 1 of the '698 patent is representative of claims 7, 8, and 9, and claims a code inspection system comprising a code inspection management module, a dynamic decoy system, an actuator module, and one or more sensor modules – all of which cooperate with a protected system, while insulating the protected system from malicious code. A code inspection management module monitors the protected system, while the dynamic decoy system is updated to parallel or emulate relevant portions of the protected system. The sensor modules enable the decoy system to analyze actions and results of one or more portions of the code in response to stimuli from the actuator module.

b. Claim 10 (and 19) of the '698 patent is representative of claims 14 (and 23), 15 (and 24), 16 (and 25), and 18 (and 27), and claims information storage media and a

> method for creating and maintaining a dynamic decoy system based on a protected system. The claims comprise a dynamic decoy system, code that is received with the dynamic decoy system, and sensors monitoring such code within the dynamic decoy system. The dynamic decoy system parallels or emulates potions of a protected system, and updates accordingly based on changes made to the protect system. Code is then introduced to the decoy system to simulate the operating conditions of the protected system and monitor actions and results.

In particular, the '698 patent relates to systems and methods for protection of computers and other devices from malicious code such as viruses, spyware, undesirable code, or the like (col. 1, lines 16-19). In the present complaint, Defendant's cybersecurity system and method infringe on these inventive aspects of the '698 patent. For example, Defendant's Advanced Malware Detection (code inspection system) offers restricted operating system environments (dynamic decoy systems) that simulate an entire host (protected system). Defendant's Advanced Malware Detection interacts (actuator module) with malware and observes (sensor module) every action and result. Forcepoint's Advanced Malware Detection is a code inspection system that provides a method of creating and maintaining a dynamic decoy system and storing relevant information, as claimed in the '698 patent.

10. The '698 patent overcomes shortcomings in the prior art, which could only detect previously known malicious code contained in a "library" of known code (col. 1, lines 59-67), and was ineffective and inefficient in creating and maintaining "test chambers" due to the many different variations of code, malware, and operating systems (col. 2, lines 23-42). Certain of the inventive aspects of the '698 patent address the need for dynamic decoy systems that operate in combination with a code inspection system to detect and destroy both known and unknown

malware through a constantly updating "test chamber" (the decoy system) that mirrors the protected system (the true operating system) (col. 3, lines 9-44 and col. 4, lines 24-35). Such system, method, and aspects were not well-understood, routine, or conventional at the time of the invention.

FORCEPOINT CYBERSECURITY SOFTWARE

11. On information and belief, Defendant provides data security, web security, email security, mobile security, data loss prevention software, insider threat protection, cloud security, network security, and cross domain solutions. In particular, Forcepoint's Advanced Malware Detection product provides an isolation and code inspection environment that simulates an entire host including the CPU, system memory and all devices. The Advanced Malware Detection product integrates with Forcepoint's firewall, web security, email security and cloud access security products, among others. For the purposes of this complaint, the term "Forcepoint Cybersecurity Software" encompasses all such code inspection and isolation functionalities and any related or integrated Forcepoint security technologies and software.

COUNT I
PATENT INFRINGEMENT OF THE '698 PATENT

12. Plaintiff Invicta repeats and realleges the above paragraphs, which are incorporated by reference as if fully restated herein.

13. Plaintiff Invicta is the owner of all rights, title, and interest in the '698 patent.

14. Plaintiff Invicta has never licensed to the Defendant under the '698 patent, nor has Plaintiff Invicta otherwise authorized the Defendant to practice any part of the '698 patent.

15. The '698 patent is presumed valid under 35 U.S.C. §282.

16. The '698 patent relates to, among other things, systems and methods for creating a code inspection system.

17. On information and belief, Defendant offers a code inspection system that simulates an entire host, including the CPU, system memory, and all devices.

18. **Direct Infringement:** On information and belief, Defendant has directly infringed and continues to directly infringe, either literally or under the doctrine of equivalents, one or more claims of the ‘698 patent, including for example (but not limited to) at least code inspection system (claims 1-9), methods of creating and maintaining such a system (claims 10-18), and information storage media for creating and maintaining such a system (claims 19-27) of the ‘698 patent by making, using, distributing, providing, supplying, selling, offering to sell without license or authority Defendant’s software that include infringing features. The infringing products include malware detection software that simulates an entire host for isolation and inspection. A detailed infringement claim mapping is provided in paragraphs 23-65.

19. **Induced Infringement:** On information and belief, Defendant has and continues to promote, advertise, and support customers/users of its Cybersecurity Software, with actions to include, but not limited to the following:

(i) Defendant’s advertising Forcepoint Cybersecurity Software, for example its Advanced Malware Detection, on its website <https://www.forcepoint.com/product/add-on/advanced-malware-detection>;

(ii) Defendant’s providing brochures, data sheets, blog posts and webcasts to potential customers from its website <https://www.forcepoint.com/resources/webcasts/detecting-evasive-malware-forcepoint-advanced-malware-detection-amd>, <https://www.forcepoint.com/blog/insights/forcepoint-reveals-casb-uba-enhanced-cloud-app-controls-and-availability-most>,

<https://www.forcepoint.com/sites/default/files/resources/files/datasheet_forcepoint_advanced_malware_detection_lastline_en_0.pdf>;

(iii) Defendant's providing technical support from its website <https://support.forcepoint.com/DocumentsDisplayed?version=1.1&name=Advanced%20Malware%20Detection%20On-Premises>, and also providing detailed technical documentation regarding installing, operating, and troubleshooting the software <https://help.stonesoft.com/onlinehelp/StoneGate/SMC/6.2.0/GUID-EECA15DA-9B8A-4C2F-9C42-D53516ADC19E.html>; and

(iv) Defendant's providing an extensive partner/reseller program for selling and supporting the software < https://www.forcepoint.com/partners/find-a-partner>.

Defendant controls the distribution and implementation of the software, whereby Defendant's software applications require the customer/user to download and install the requisite software, either on a customer's servers or via a cloud-based installation. On information and belief, Defendant continues to engage in these acts with knowledge of the '698 patent by the filing of this Complaint, and with the actual intent to cause the acts which it knew or should have known would induce actual infringement.

20. Defendant Forcepoint has infringed the '698 patent by making, having made, using, importing, providing, supplying, distributing, selling, or offering for sale code inspection systems utilizing methods for creating and maintaining a dynamic decoy system, and related information storage media.

21. The '698 patent is well known in the industry – having been cited in at least 80 cited patents since its filing date.

22. **Detailed Mapping of Direct Infringement:** On information and belief, infringement of the '698 patent by Forcepoint products and software as demonstrated below.

23. Code inspection system claim 1 of the alleged claims:

1. A code inspection system comprising:

a code inspection management module that monitors and communicates with a protected system;

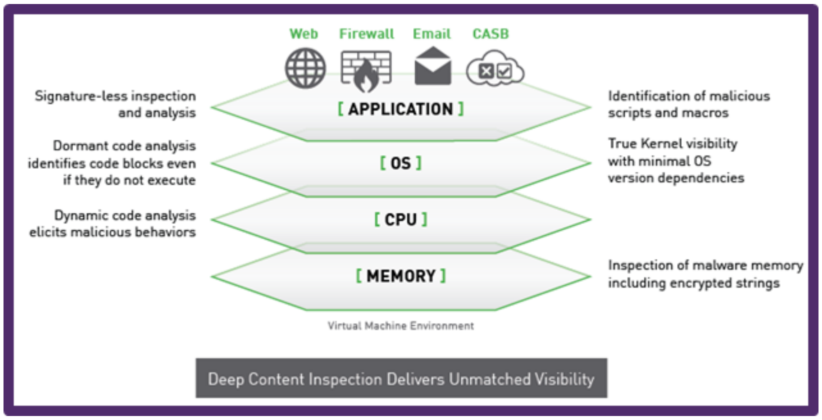
a dynamic decoy system that, in cooperation with the code inspection management module, is updated to substantially parallel relevant portions of the protected system;

an actuator module; and

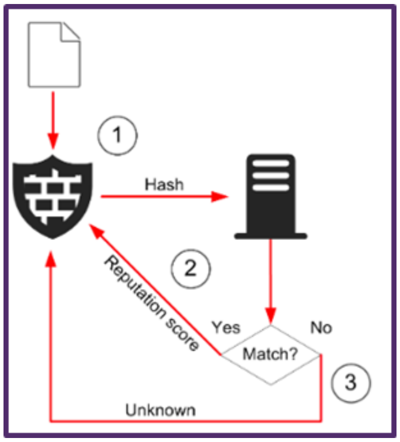
one or more sensor modules, wherein the dynamic decoy system is capable of analyzing at least one of actions and results of one or more portions of code in response to stimuli from the actuator module,

wherein the relevant portions of the protected system allow the one or more portions of code to be analyzed in the dynamic decoy system as if the dynamic decoy system were the protected system.

24. On information and belief, Forcepoint Cybersecurity Software is a code inspection system.

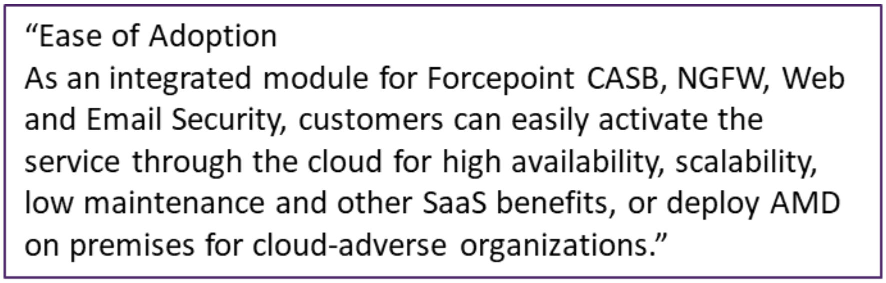

Web
Firewall
Email
CASB
Signature-less inspection and analysis
Dormant code analysis identifies code blocks even if they do not execute
Dynamic code analysis elicits malicious behaviors
[APPLICATION]
[OS]
[CPU]
[MEMORY]
Virtual Machine Environment
Identification of malicious scripts and macros
True Kernel visibility with minimal OS version dependencies
Inspection of malware memory including encrypted strings
Deep Content Inspection Delivers Unmatched Visibility

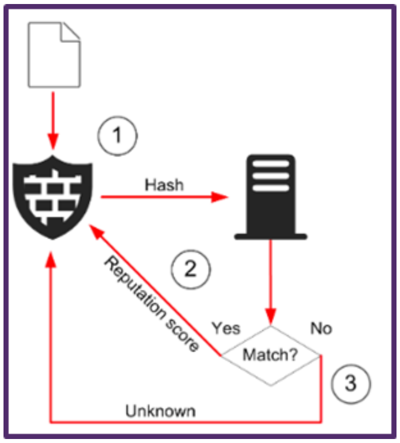
https://www.forcepoint.com/product/add-on/advanced-malware-detection

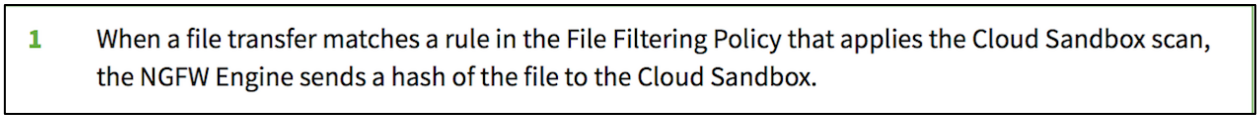


https://help.stonesoft.com/onlinehelp/StoneGate/SMC/6.4.0/GUID-EECA15DA-9B8A-4C2F-9C42-D53516ADC19E.html

25. On information and belief, Forcepoint Cybersecurity Software contains a code inspection management module that monitors and communicates with a protected system.

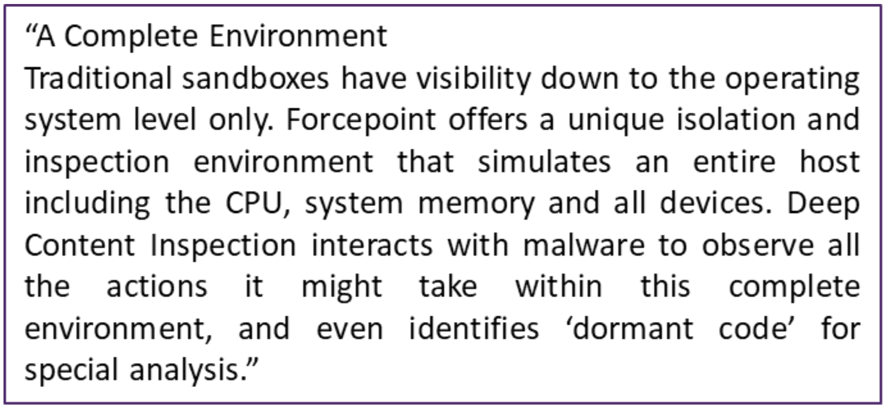

"Ease of Adoption
As an integrated module for Forcepoint CASB, NGFW, Web and Email Security, customers can easily activate the service through the cloud for high availability, scalability, low maintenance and other SaaS benefits, or deploy AMD on premises for cloud-adverse organizations."




1 When a file transfer matches a rule in the File Filtering Policy that applies the Cloud Sandbox scan, the NGFW Engine sends a hash of the file to the Cloud Sandbox.

https://help.stonesoft.com/onlinehelp/StoneGate/SMC/6.4.0/GUID-EECA15DA-9B8A-4C2F-9C42-D53516ADC19E.html

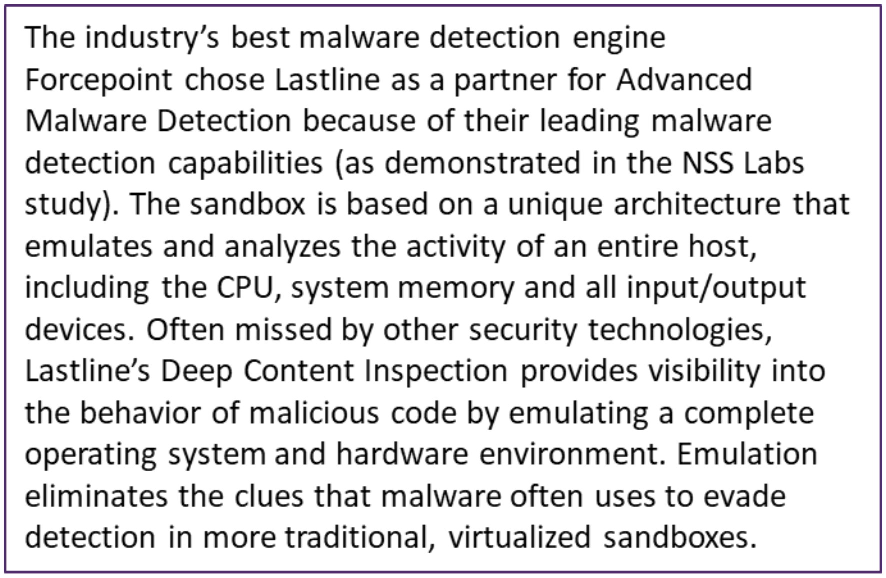
26. On information and belief, Forcepoint Cybersecurity Software contains a dynamic decoy system that, in cooperation with the code inspection management module, is updated to substantially parallel relevant portions of the protected system.



"A Complete Environment
Traditional sandboxes have visibility down to the operating system level only. Forcepoint offers a unique isolation and inspection environment that simulates an entire host including the CPU, system memory and all devices. Deep Content Inspection interacts with malware to observe all the actions it might take within this complete environment, and even identifies 'dormant code' for special analysis."

https://www.forcepoint.com/product/add-on/advanced-malware-detection

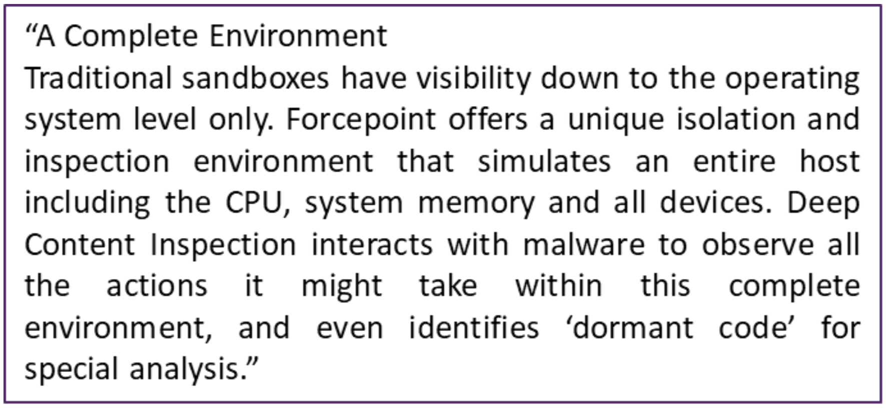
27. On information and belief, Forcepoint Cybersecurity Software contains an actuator module.



The industry's best malware detection engine
Forcepoint chose Lastline as a partner for Advanced Malware Detection because of their leading malware detection capabilities (as demonstrated in the NSS Labs study). The sandbox is based on a unique architecture that emulates and analyzes the activity of an entire host, including the CPU, system memory and all input/output devices. Often missed by other security technologies, Lastline's Deep Content Inspection provides visibility into the behavior of malicious code by emulating a complete operating system and hardware environment. Emulation eliminates the clues that malware often uses to evade detection in more traditional, virtualized sandboxes.

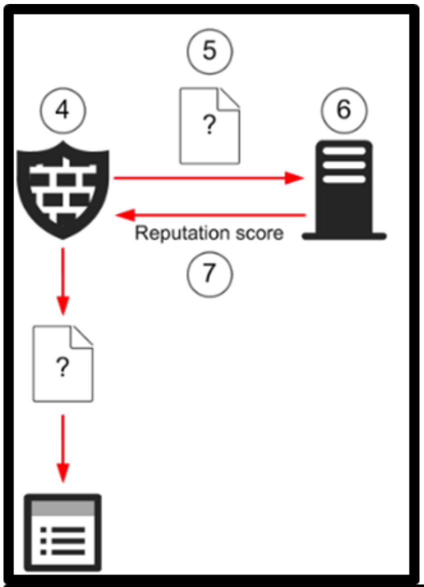
https://www.forcepoint.com/sites/default/files/resources/files/datasheet_forcepoint_advanced_malware_detection_lastline_en_0.pdf

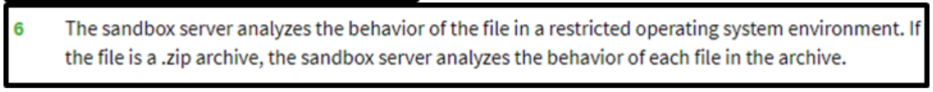
28. On information and belief, Forcepoint Cybersecurity Software contains one or more sensor modules, wherein the dynamic decoy system is capable of analyzing at least one of actions and results of one or more portions of code in response to stimuli from the actuator module.



"A Complete Environment
Traditional sandboxes have visibility down to the operating system level only. Forcepoint offers a unique isolation and inspection environment that simulates an entire host including the CPU, system memory and all devices. Deep Content Inspection interacts with malware to observe all the actions it might take within this complete environment, and even identifies 'dormant code' for special analysis."

https://www.forcepoint.com/product/add-on/advanced-malware-detection

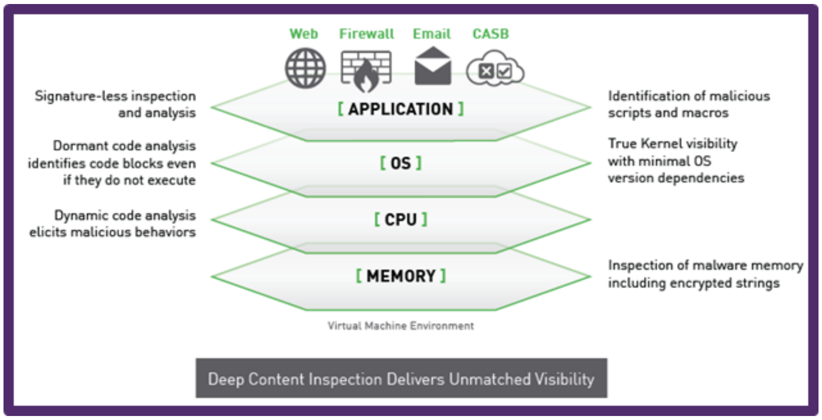




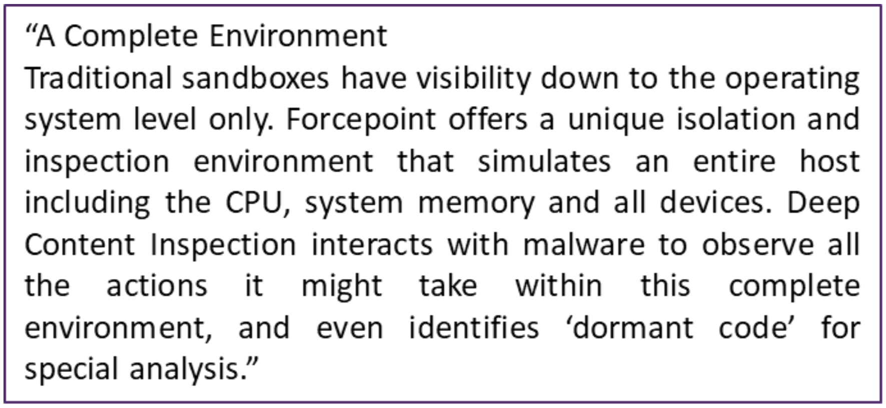
6 The sandbox server analyzes the behavior of the file in a restricted operating system environment. If the file is a .zip archive, the sandbox server analyzes the behavior of each file in the archive.

https://help.stonesoft.com/onlinehelp/StoneGate/SMC/6.4.0/GUID-EECA15DA-9B8A-4C2F-9C42-D53516ADC19E.html

29. On information and belief, the relevant portions of Forcepoint Cybersecurity Software allow the one or more portions of code to be analyzed in the dynamic decoy system as if the dynamic decoy system were the protected system.


Web
Firewall
Email
CASB
Signature-less inspection and analysis
Dormant code analysis identifies code blocks even if they do not execute
Dynamic code analysis elicits malicious behaviors
[APPLICATION]
[OS]
[CPU]
[MEMORY]
Virtual Machine Environment
Identification of malicious scripts and macros
True Kernel visibility with minimal OS version dependencies
Inspection of malware memory including encrypted strings
Deep Content Inspection Delivers Unmatched Visibility

https://www.forcepoint.com/product/add-on/advanced-malware-detection



"A Complete Environment
Traditional sandboxes have visibility down to the operating system level only. Forcepoint offers a unique isolation and inspection environment that simulates an entire host including the CPU, system memory and all devices. Deep Content Inspection interacts with malware to observe all the actions it might take within this complete environment, and even identifies 'dormant code' for special analysis."

https://www.forcepoint.com/product/add-on/advanced-malware-detection

30. Code inspection system claim 7 of the alleged claims:

7. A code inspection system comprising:

a code inspection management module that monitors and communicates with a protected system;

a dynamic decoy system that, in cooperation with the code inspection management module, is updated to substantially parallel relevant portions of the protected system;

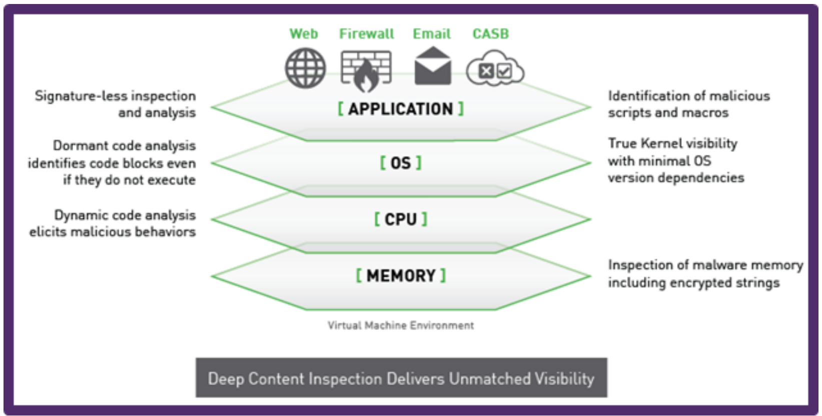
an actuator module; and

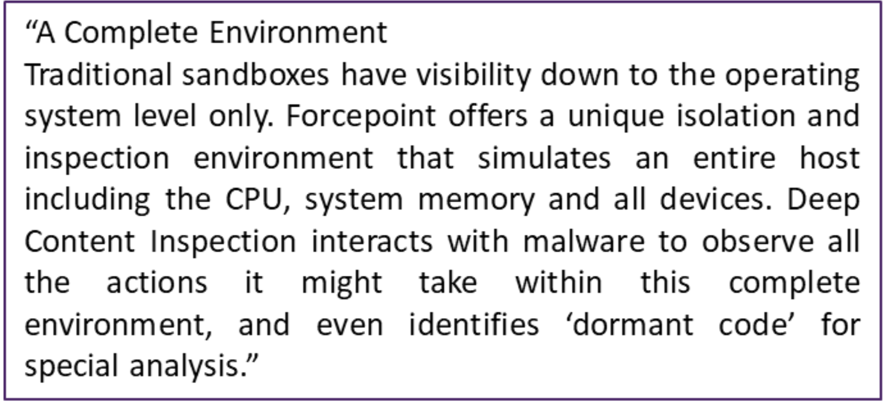
one or more sensor modules, wherein the dynamic decoy system is capable of analyzing at least one of actions and results of one or more portions of code in response to stimuli from the actuator module,

wherein at least a portion of the protected system is capable of being recovered from the dynamic decoy system.

31. Plaintiff Invicta repeats and realleges paragraphs 24 through 28 as representative of the code inspection system elements of claim 7, including a code inspection management module, a dynamic decoy system, an actuator module, and sensor modules.

32. On information and belief, at least a portion of Forcepoint Cybersecurity Software is capable of being recovered from the dynamic decoy system.


Web
Firewall
Email
CASB
Signature-less inspection and analysis
[APPLICATION]
Identification of malicious scripts and macros
Dormant code analysis identifies code blocks even if they do not execute
[OS]
True Kernel visibility with minimal OS version dependencies
Dynamic code analysis elicits malicious behaviors
[CPU]
[MEMORY]
Inspection of malware memory including encrypted strings
Virtual Machine Environment
Deep Content Inspection Delivers Unmatched Visibility


"A Complete Environment
Traditional sandboxes have visibility down to the operating system level only. Forcepoint offers a unique isolation and inspection environment that simulates an entire host including the CPU, system memory and all devices. Deep Content Inspection interacts with malware to observe all the actions it might take within this complete environment, and even identifies 'dormant code' for special analysis."

https://www.forcepoint.com/product/add-on/advanced-malware-detection

33. Code inspection system claim 8 of the alleged claims:

8. A code inspection system comprising:

a code inspection management module that monitors and communicates with a protected system;

a dynamic decoy system that, in cooperation with the code inspection management module, is updated to substantially parallel relevant portions of the protected system;

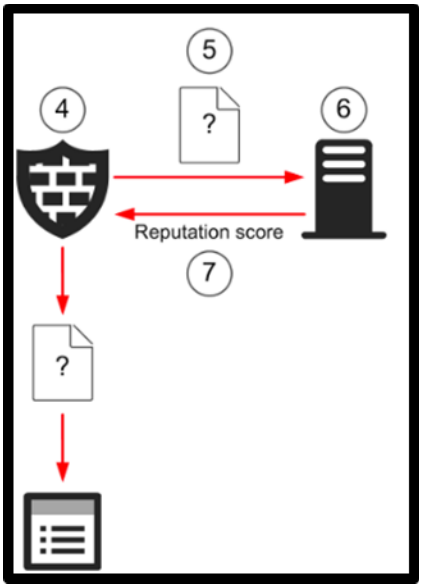
an actuator module; and

one or more sensor modules, wherein the dynamic decoy system is capable of analyzing at least one of actions and results of one or more portions of code in response to stimuli from the actuator module,

wherein the code inspection system is an interface between the protected system and one or more unprotected systems.

34. Plaintiff Invicta repeats and realleges paragraphs 24 through 28 as representative of the code inspection system elements of claim 8, including a code inspection management module, a dynamic decoy system, an actuator module, and sensor modules.

35. On information and belief, the Forcepoint Cybersecurity Software is an interface between the protected system and one or more unprotected systems.



5 If the file has not previously been analyzed, the NGFW Engine uploads a copy of the unknown file to the sandbox server. If any of the files in a .zip archive have not previously been analyzed, the NGFW Engine uploads a copy of the whole .zip archive to the sandbox server.

https://www.forcepoint.com/product/add-on/advanced-malware-detection

36. Code inspection system claim 9 of the alleged claims:

9. A code inspection system comprising:

a code inspection management module that monitors and communicates with a protected system;

a dynamic decoy system that, in cooperation with the code inspection management module, is updated to substantially parallel relevant portions of the protected system;

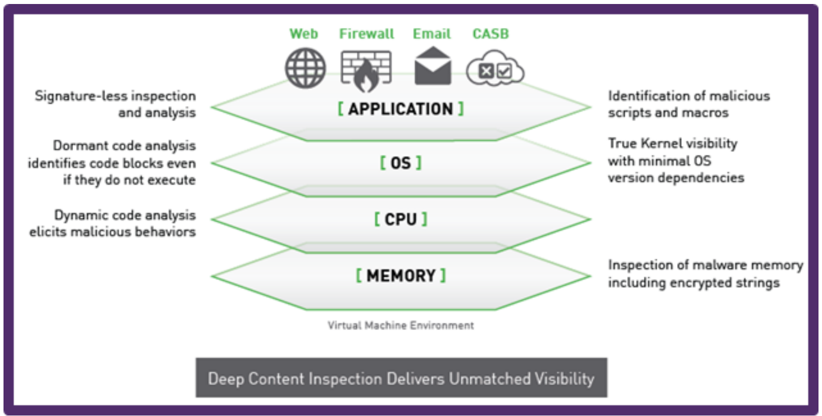
an actuator module; and

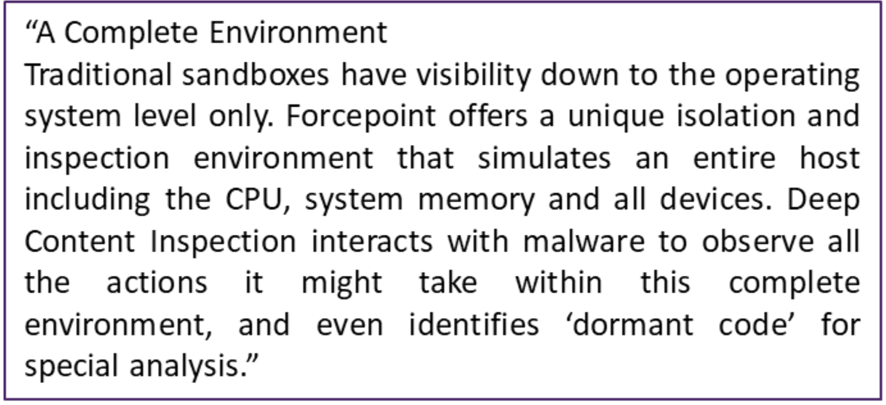
one or more sensor modules, wherein the dynamic decoy system is capable of analyzing at least one of actions and results of one or more portions of code in response to stimuli from the actuator module,

wherein the code inspection management module monitors the protected system and updates the dynamic decoy system based on at least one of installed software, installed hardware, operating system upgrades, software upgrades, hardware upgrades, software deletions, hardware deletions and input/output devices.

37. Plaintiff Invicta repeats and realleges paragraphs 24 through 28 as representative of the code inspection system elements of claim 9, including a code inspection management module, a dynamic decoy system, an actuator module, and sensor modules.

38. On information and belief, Forcepoint Cybersecurity Software monitors the protected system and updates the dynamic decoy system based on at least one of installed software, installed hardware, operating system upgrades, software upgrades, hardware upgrades, software deletions, hardware deletions and input/output devices.


Web
Firewall
Email
CASB
Signature-less inspection and analysis
Dormant code analysis identifies code blocks even if they do not execute
Dynamic code analysis elicits malicious behaviors
[APPLICATION]
[OS]
[CPU]
[MEMORY]
Virtual Machine Environment
Identification of malicious scripts and macros
True Kernel visibility with minimal OS version dependencies
Inspection of malware memory including encrypted strings
Deep Content Inspection Delivers Unmatched Visibility


"A Complete Environment
Traditional sandboxes have visibility down to the operating system level only. Forcepoint offers a unique isolation and inspection environment that simulates an entire host including the CPU, system memory and all devices. Deep Content Inspection interacts with malware to observe all the actions it might take within this complete environment, and even identifies 'dormant code' for special analysis."

https://www.forcepoint.com/product/add-on/advanced-malware-detection

39. Method claim 10 of the alleged claims:

10. A method of creating and maintaining a dynamic decoy system based on a protected system comprising:
creating a dynamic decoy system that substantially parallels relevant portions of a protected system;
updating the dynamic decoy system based on changes to the protected system;
receiving one or more portions of code;

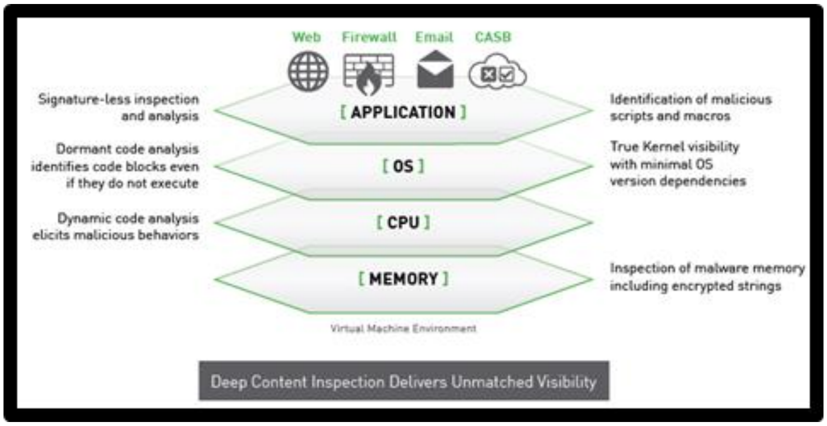
introducing the one or more portions of code to the dynamic decoy system;

simulating operating conditions of the protected system in the dynamic decoy system; and

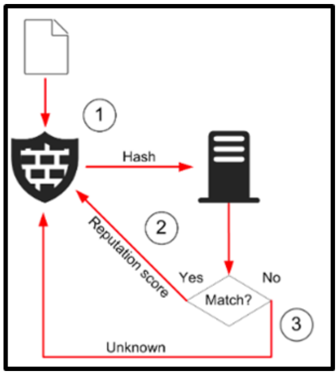
monitoring sensors in the dynamic decoy system for at least one of actions or results of the one or more portions of code,

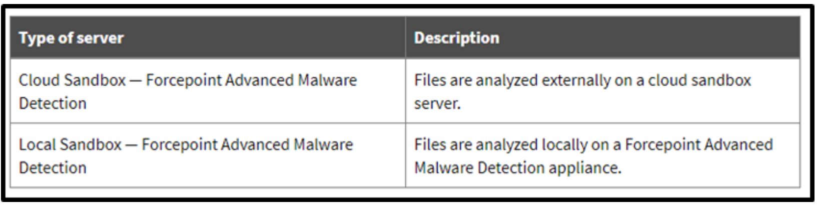
wherein the relevant portions of the protected system allow the one or more portions of code to be analyzed in the dynamic decoy system as if the dynamic decoy system were the protected system.

40. On information and belief, Forcepoint Cybersecurity Software conducts a method of creating and maintaining a dynamic decoy system based on a protected system.


Web
Firewall
Email
CASB
Signature-less inspection and analysis
[APPLICATION]
Identification of malicious scripts and macros
Dormant code analysis identifies code blocks even if they do not execute
[OS]
True Kernel visibility with minimal OS version dependencies
Dynamic code analysis elicits malicious behaviors
[CPU]
[MEMORY]
Inspection of malware memory including encrypted strings
Virtual Machine Environment
Deep Content Inspection Delivers Unmatched Visibility

https://www.forcepoint.com/product/add-on/advanced-malware-detection

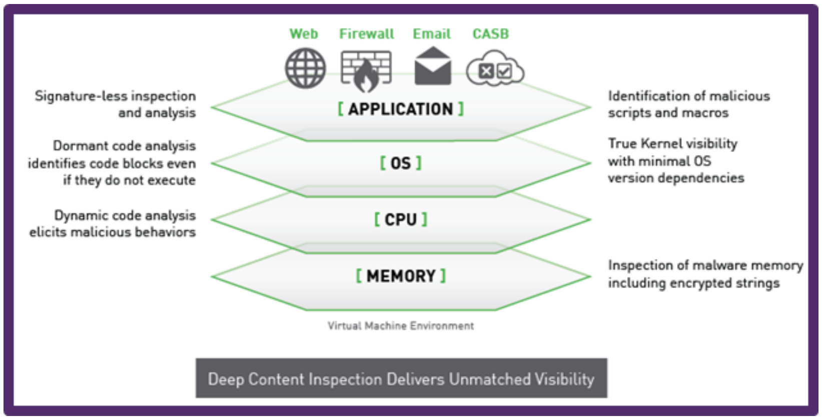


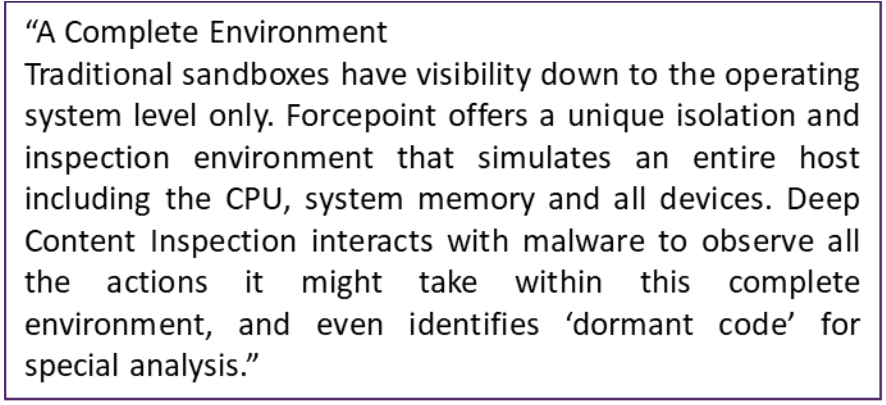


Type of server	Description
Cloud Sandbox — Forcepoint Advanced Malware Detection	Files are analyzed externally on a cloud sandbox server.
Local Sandbox — Forcepoint Advanced Malware Detection	Files are analyzed locally on a Forcepoint Advanced Malware Detection appliance.

https://help.stonesoft.com/onlinehelp/StoneGate/SMC/6.4.0/GUID-EECA15DA-9B8A-4C2F-9C42-D53516ADC19E.html

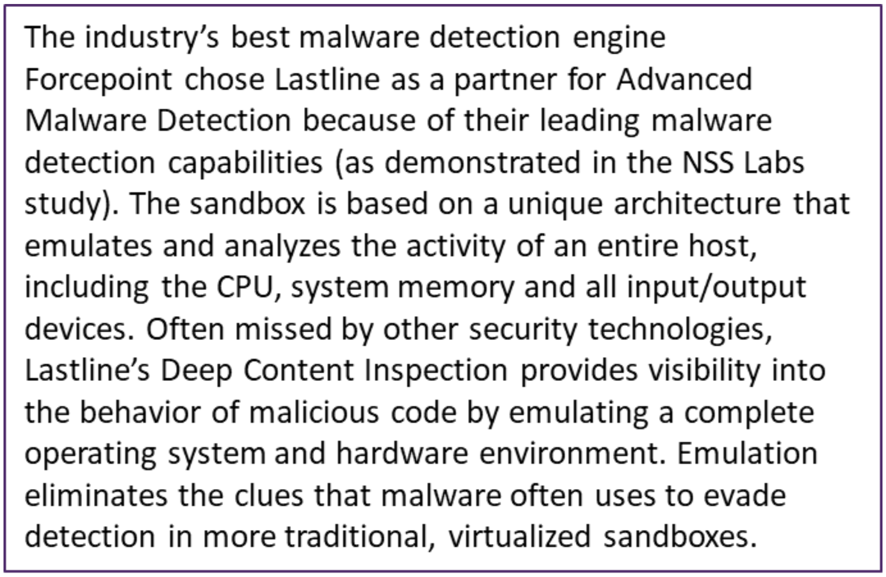
41. On information and belief, Forcepoint Cybersecurity Software creates a dynamic decoy system that substantially parallels relevant portions of a protected system.


Web
Firewall
Email
CASB
[APPLICATION]
[OS]
[CPU]
[MEMORY]
Virtual Machine Environment
Signature-less inspection and analysis
Dormant code analysis identifies code blocks even if they do not execute
Dynamic code analysis elicits malicious behaviors
Identification of malicious scripts and macros
True Kernel visibility with minimal OS version dependencies
Inspection of malware memory including encrypted strings
Deep Content Inspection Delivers Unmatched Visibility


"A Complete Environment
Traditional sandboxes have visibility down to the operating system level only. Forcepoint offers a unique isolation and inspection environment that simulates an entire host including the CPU, system memory and all devices. Deep Content Inspection interacts with malware to observe all the actions it might take within this complete environment, and even identifies 'dormant code' for special analysis."

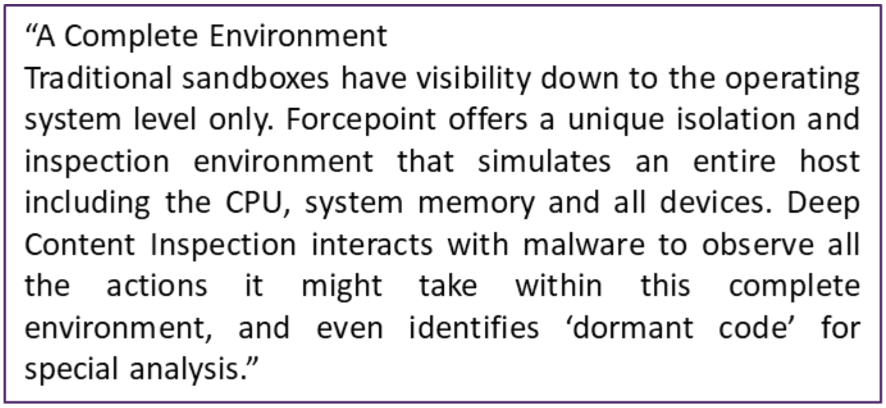
https://www.forcepoint.com/product/add-on/advanced-malware-detection

42. On information and belief, Forcepoint Cybersecurity Software updates the dynamic decoy system based on changes to the protected system.


The industry's best malware detection engine
Forcepoint chose Lastline as a partner for Advanced Malware Detection because of their leading malware detection capabilities (as demonstrated in the NSS Labs study). The sandbox is based on a unique architecture that emulates and analyzes the activity of an entire host, including the CPU, system memory and all input/output devices. Often missed by other security technologies, Lastline's Deep Content Inspection provides visibility into the behavior of malicious code by emulating a complete operating system and hardware environment. Emulation eliminates the clues that malware often uses to evade detection in more traditional, virtualized sandboxes.

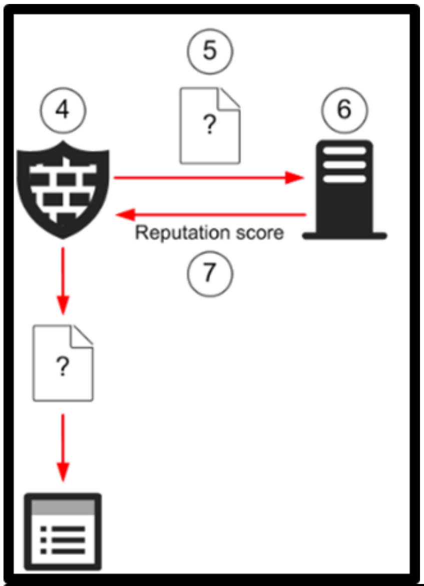
https://www.forcepoint.com/sites/default/files/resources/files/datasheet_forcepoint_advanced_malware_detection_lastline_en_0.pdf

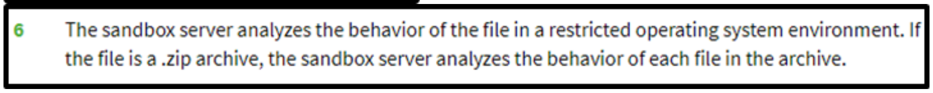
43. On information and belief, Forcepoint Cybersecurity Software receives one or more portions of code.



"A Complete Environment
Traditional sandboxes have visibility down to the operating system level only. Forcepoint offers a unique isolation and inspection environment that simulates an entire host including the CPU, system memory and all devices. Deep Content Inspection interacts with malware to observe all the actions it might take within this complete environment, and even identifies 'dormant code' for special analysis."

https://www.forcepoint.com/product/add-on/advanced-malware-detection

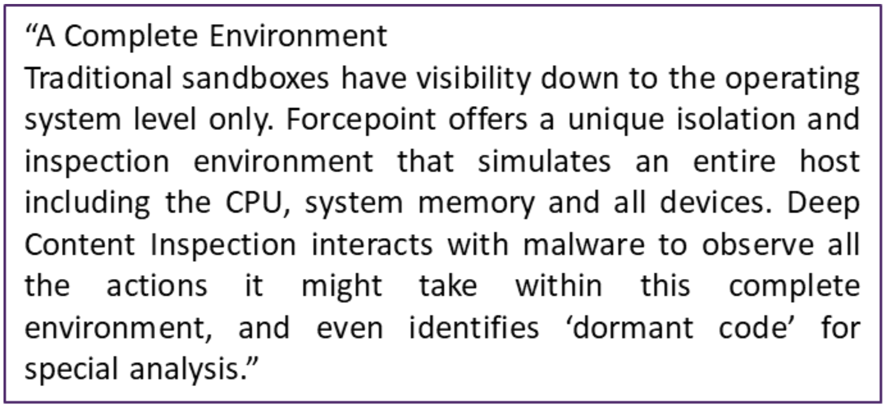




6 The sandbox server analyzes the behavior of the file in a restricted operating system environment. If the file is a .zip archive, the sandbox server analyzes the behavior of each file in the archive.

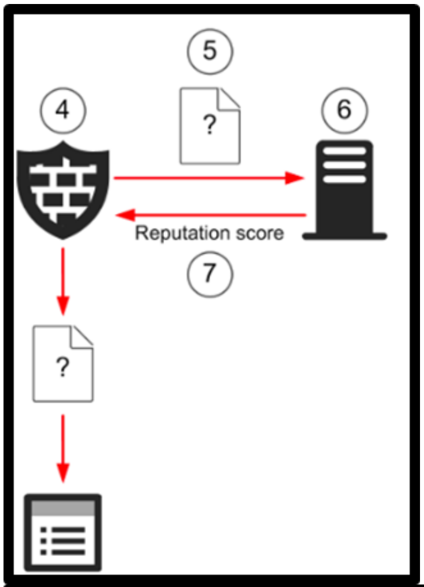
https://help.stonesoft.com/onlinehelp/StoneGate/SMC/6.4.0/GUID-EECA15DA-9B8A-4C2F-9C42-D53516ADC19E.html

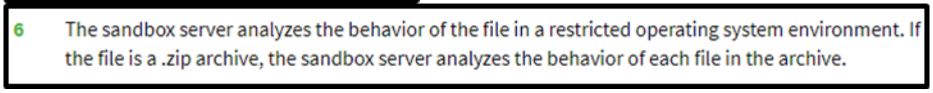
44. On information and belief, Forcepoint Cybersecurity Software introduces the one or more portions of code to the dynamic decoy system.



"A Complete Environment
Traditional sandboxes have visibility down to the operating system level only. Forcepoint offers a unique isolation and inspection environment that simulates an entire host including the CPU, system memory and all devices. Deep Content Inspection interacts with malware to observe all the actions it might take within this complete environment, and even identifies 'dormant code' for special analysis."

https://www.forcepoint.com/product/add-on/advanced-malware-detection

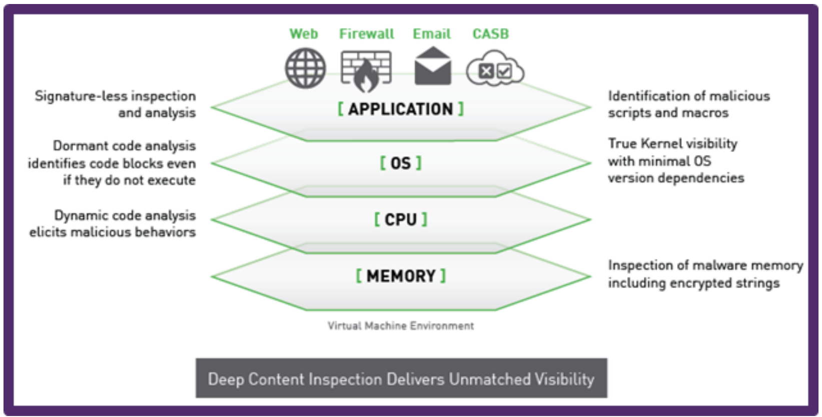




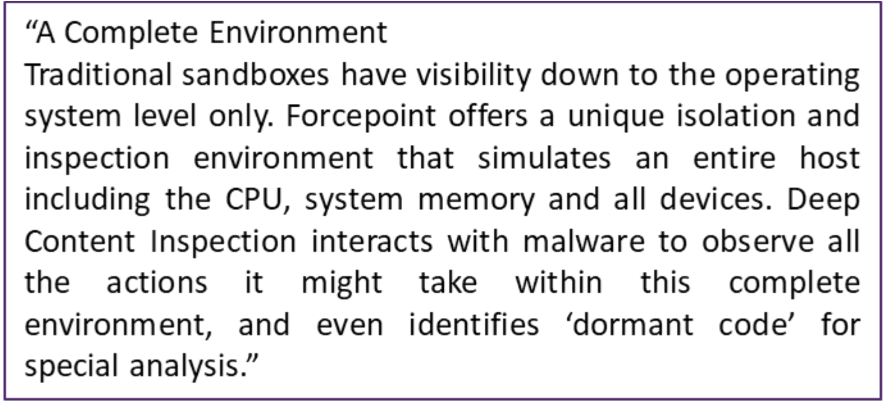
6 The sandbox server analyzes the behavior of the file in a restricted operating system environment. If the file is a .zip archive, the sandbox server analyzes the behavior of each file in the archive.

https://help.stonesoft.com/onlinehelp/StoneGate/SMC/6.4.0/GUID-EECA15DA-9B8A-4C2F-9C42-D53516ADC19E.html

45. On information and belief, Forcepoint Cybersecurity Software simulates operating conditions of the protected system in the dynamic decoy system.

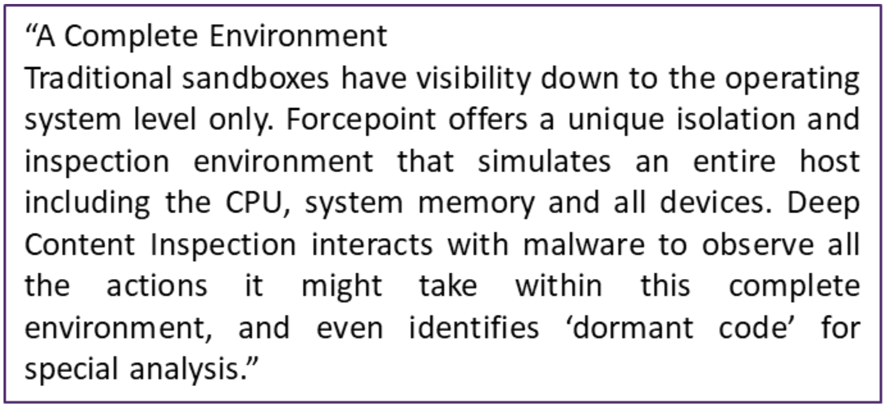

Web
Firewall
Email
CASB
[APPLICATION]
[OS]
[CPU]
[MEMORY]
Virtual Machine Environment
Signature-less inspection and analysis
Dormant code analysis identifies code blocks even if they do not execute
Dynamic code analysis elicits malicious behaviors
Identification of malicious scripts and macros
True Kernel visibility with minimal OS version dependencies
Inspection of malware memory including encrypted strings

Deep Content Inspection Delivers Unmatched Visibility

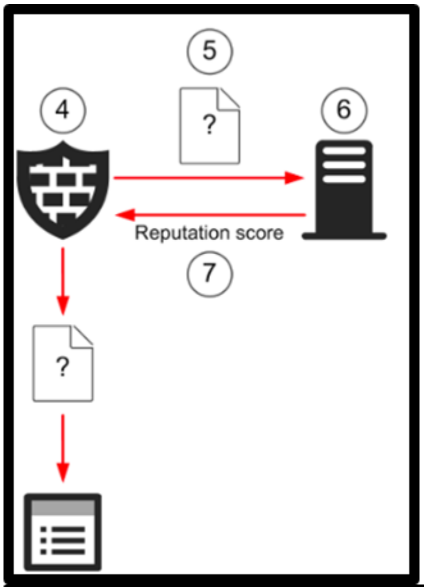

"A Complete Environment
Traditional sandboxes have visibility down to the operating system level only. Forcepoint offers a unique isolation and inspection environment that simulates an entire host including the CPU, system memory and all devices. Deep Content Inspection interacts with malware to observe all the actions it might take within this complete environment, and even identifies 'dormant code' for special analysis."

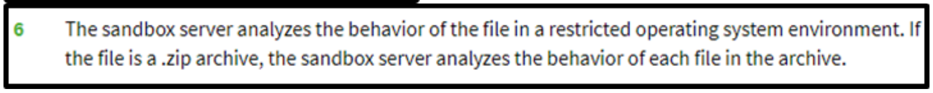
https://www.forcepoint.com/product/add-on/advanced-malware-detection

46. On information and belief, Forcepoint Cybersecurity Software monitors sensors in the dynamic decoy system for at least one of actions or results of the one or more portions of code.


"A Complete Environment
Traditional sandboxes have visibility down to the operating system level only. Forcepoint offers a unique isolation and inspection environment that simulates an entire host including the CPU, system memory and all devices. Deep Content Inspection interacts with malware to observe all the actions it might take within this complete environment, and even identifies 'dormant code' for special analysis."

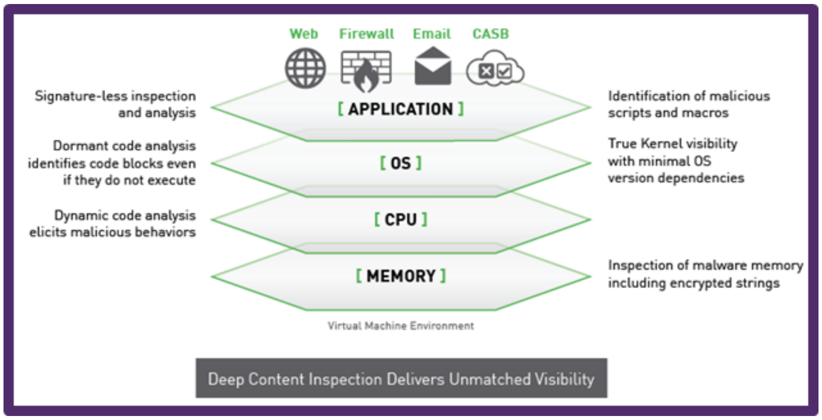
https://www.forcepoint.com/product/add-on/advanced-malware-detection



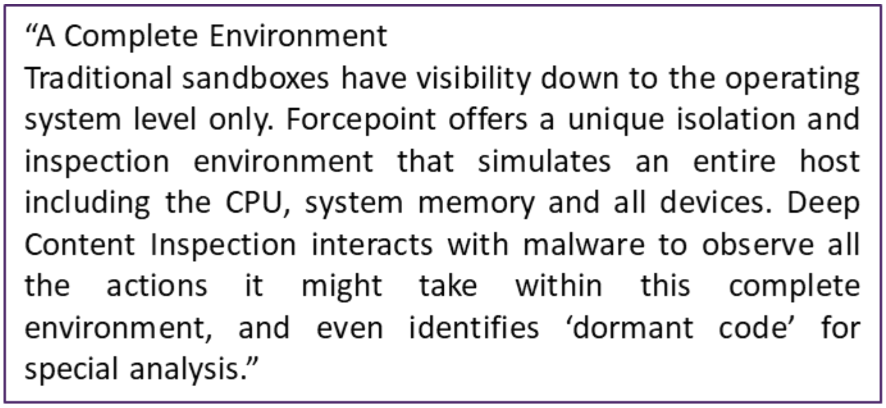

6 The sandbox server analyzes the behavior of the file in a restricted operating system environment. If the file is a .zip archive, the sandbox server analyzes the behavior of each file in the archive.

https://help.stonesoft.com/onlinehelp/StoneGate/SMC/6.4.0/GUID-EECA15DA-9B8A-4C2F-9C42-D53516ADC19E.html

47. On information and belief, relevant portions of Forcepoint Cybersecurity Software allow the one or more portions of code to be analyzed in the dynamic decoy system as if the dynamic decoy system were the protected system.


Web
Firewall
Email
CASB
Signature-less inspection and analysis
[APPLICATION]
Identification of malicious scripts and macros
Dormant code analysis identifies code blocks even if they do not execute
[OS]
True Kernel visibility with minimal OS version dependencies
Dynamic code analysis elicits malicious behaviors
[CPU]
[MEMORY]
Inspection of malware memory including encrypted strings
Virtual Machine Environment
Deep Content Inspection Delivers Unmatched Visibility

https://www.forcepoint.com/product/add-on/advanced-malware-detection



"A Complete Environment
Traditional sandboxes have visibility down to the operating system level only. Forcepoint offers a unique isolation and inspection environment that simulates an entire host including the CPU, system memory and all devices. Deep Content Inspection interacts with malware to observe all the actions it might take within this complete environment, and even identifies 'dormant code' for special analysis."

https://www.forcepoint.com/product/add-on/advanced-malware-detection

48. Method claim 14 of the alleged claims:

14. A method of creating and maintaining a dynamic decoy system based on a protected system comprising:

creating a dynamic decoy system that substantially parallels relevant portions of a protected system;

updating the dynamic decoy system based on changes to the protected system;

receiving one or more portions of code;

introducing the one or more portions of code to the dynamic decoy system;

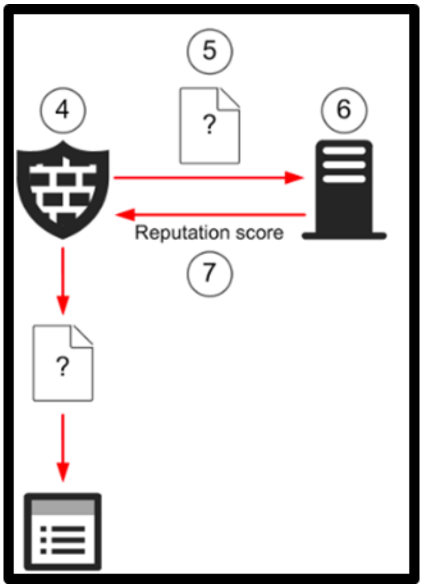
simulating operating conditions of the protected system in the dynamic decoy system;

and monitoring sensors in the dynamic decoy system for at least one of actions or results of the one or more portions of code,

wherein the dynamic decoy system is an interface between the protected system and one or more unprotected systems.

49. Plaintiff Invicta repeats and realleges paragraphs 40 through 46 as representative of the method steps of claim 14, including creating a dynamic decoy system, updating the system, receiving and introducing portions of code into the system, simulating operating conditions, and monitoring sensors in the system.

50. On information and belief, Forcepoint Cybersecurity Software is an interface between the protected system and one or more unprotected systems.



5 If the file has not previously been analyzed, the NGFW Engine uploads a copy of the unknown file to the sandbox server. If any of the files in a .zip archive have not previously been analyzed, the NGFW Engine uploads a copy of the whole .zip archive to the sandbox server.

https://www.forcepoint.com/product/add-on/advanced-malware-detection

51. Method claim 15 of the alleged claims:

15. A method of creating and maintaining a dynamic decoy system based on a protected system comprising:

creating a dynamic decoy system that substantially parallels relevant portions of a protected system;

updating the dynamic decoy system based on changes to the protected system;

receiving one or more portions of code;

introducing the one or more portions of code to the dynamic decoy system;

simulating operating conditions of the protected system in the dynamic decoy system;

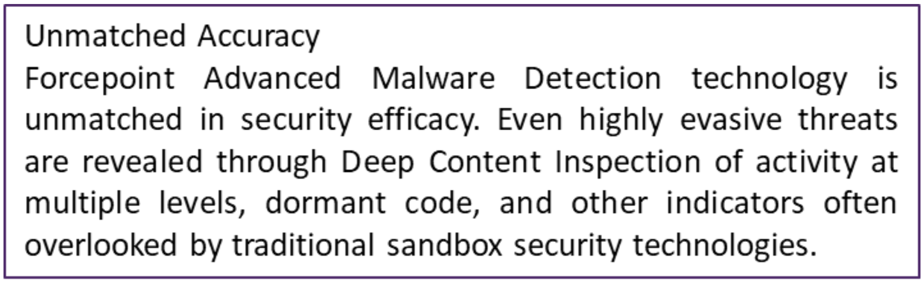
monitoring sensors in the dynamic decoy system for at least one of actions or results of the one or more portions of code; and

installing one or more sensors in the dynamic decoy system that detect one or more of unauthorized access attempts, unauthorized command execution attempts and unauthorized modifications to one or more portions of the dynamic decoy machine.

52. Plaintiff Invicta repeats and realleges paragraphs 40 through 46 as representative of the method steps of claim 15, including creating a dynamic decoy system, updating the system, receiving and introducing portions of code into the system, simulating operating conditions, and monitoring sensors in the system.

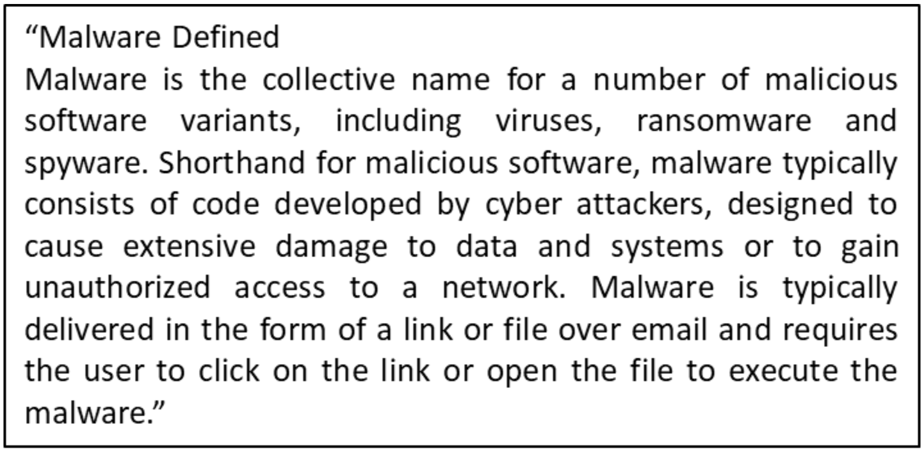
53. On information and belief, Forcepoint Cybersecurity Software installs one or more sensors in the dynamic decoy system that detect one or more of unauthorized access attempts,

unauthorized command execution attempts and unauthorized modifications to one or more portions of the dynamic decoy machine.



Unmatched Accuracy
Forcepoint Advanced Malware Detection technology is unmatched in security efficacy. Even highly evasive threats are revealed through Deep Content Inspection of activity at multiple levels, dormant code, and other indicators often overlooked by traditional sandbox security technologies.

https://www.forcepoint.com/product/add-on/advanced-malware-detection



"Malware Defined
Malware is the collective name for a number of malicious software variants, including viruses, ransomware and spyware. Shorthand for malicious software, malware typically consists of code developed by cyber attackers, designed to cause extensive damage to data and systems or to gain unauthorized access to a network. Malware is typically delivered in the form of a link or file over email and requires the user to click on the link or open the file to execute the malware."

https://www.forcepoint.com/cyber-edu/malware

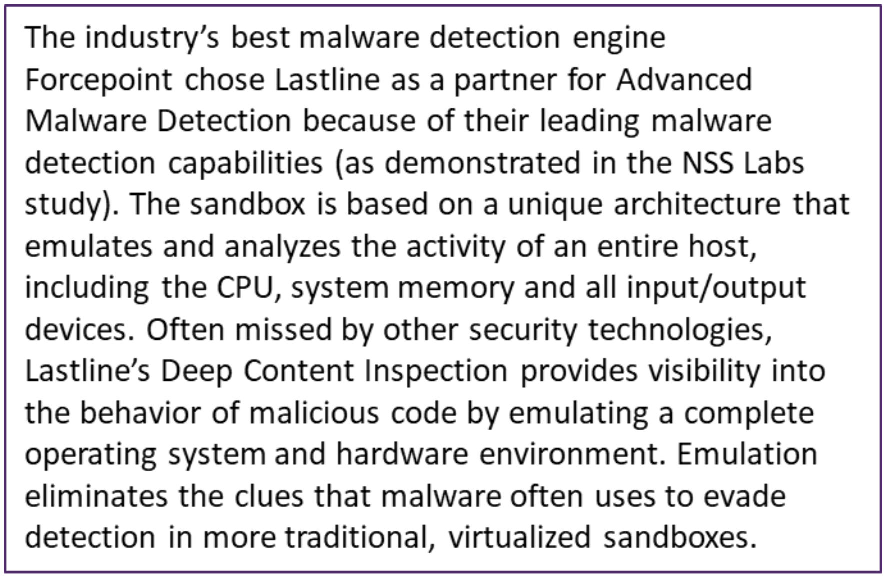
54. Method claim 16 of the alleged claims:

16. A method of creating and maintaining a dynamic decoy system based on a protected system comprising:
creating a dynamic decoy system that substantially parallels relevant portions of a protected system;
updating the dynamic decoy system based on changes to the protected system;
receiving one or more portions of code;
introducing the one or more portions of code to the dynamic decoy system;
simulating operating conditions of the protected system in the dynamic decoy system;
monitoring sensors in the dynamic decoy system for at least one of actions or results of the one or more portions of code; and
installing an actuator in the dynamic decoy system.

55. Plaintiff Invicta repeats and realleges paragraphs 40 through 46 as representative of the method steps of claim 16, including creating a dynamic decoy system, updating the system,

receiving and introducing portions of code into the system, simulating operating conditions, and monitoring sensors in the system.

56. On information and belief, Forcepoint Cybersecurity Software installs an actuator in the dynamic decoy system.



The industry's best malware detection engine
Forcepoint chose Lastline as a partner for Advanced Malware Detection because of their leading malware detection capabilities (as demonstrated in the NSS Labs study). The sandbox is based on a unique architecture that emulates and analyzes the activity of an entire host, including the CPU, system memory and all input/output devices. Often missed by other security technologies, Lastline's Deep Content Inspection provides visibility into the behavior of malicious code by emulating a complete operating system and hardware environment. Emulation eliminates the clues that malware often uses to evade detection in more traditional, virtualized sandboxes.

https://www.forcepoint.com/sites/default/files/resources/files/datasheet_forcepoint_advanced_malware_detection_lastline_en_0.pdf

57. Method claim 18 of the alleged claims:

18. A method of creating and maintaining a dynamic decoy system based on a protected system comprising:

creating a dynamic decoy system that substantially parallels relevant portions of a protected system;

updating the dynamic decoy system based on changes to the protected system;

receiving one or more portions of code;

introducing the one or more portions of code to the dynamic decoy system;

simulating operating conditions of the protected system in the dynamic decoy system; and

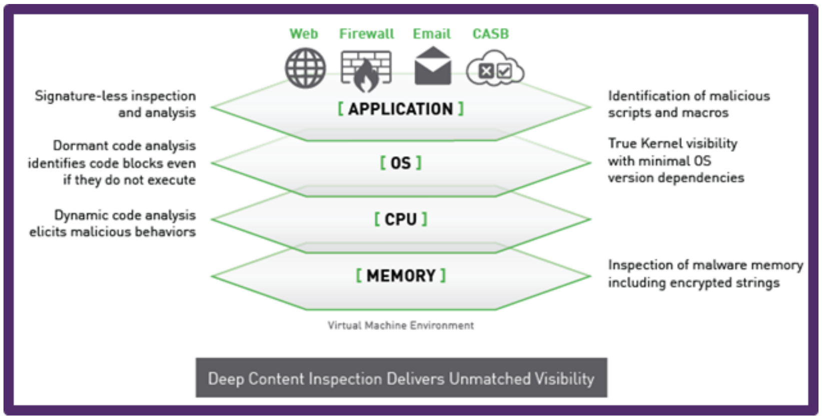
monitoring sensors in the dynamic decoy system for at least one of actions or results of the one or more portions of code,

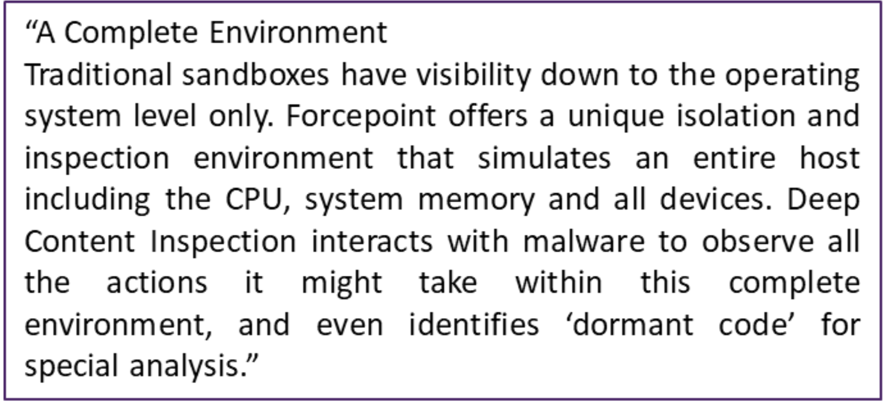
wherein updating the dynamic decoy system is based on at least one of installed software, installed hardware, operating system upgrades, software upgrades, hardware upgrades, software deletions, hardware deletions and input/output devices.

58. Plaintiff Invicta repeats and realleges paragraphs 40 through 46 as representative of the method steps of claim 18, including creating a dynamic decoy system, updating the system,

receiving and introducing portions of code into the system, simulating operating conditions, and monitoring sensors in the system.

59. On information and belief, Forcepoint Cybersecurity Software updates its dynamic decoy system based on at least one of installed software, installed hardware, operating system upgrades, software upgrades, hardware upgrades, software deletions, hardware deletions and input/output devices.


Web
Firewall
Email
CASB
Signature-less inspection and analysis
[APPLICATION]
Identification of malicious scripts and macros
Dormant code analysis identifies code blocks even if they do not execute
[OS]
True Kernel visibility with minimal OS version dependencies
Dynamic code analysis elicits malicious behaviors
[CPU]
[MEMORY]
Inspection of malware memory including encrypted strings
Virtual Machine Environment
Deep Content Inspection Delivers Unmatched Visibility


"A Complete Environment
Traditional sandboxes have visibility down to the operating system level only. Forcepoint offers a unique isolation and inspection environment that simulates an entire host including the CPU, system memory and all devices. Deep Content Inspection interacts with malware to observe all the actions it might take within this complete environment, and even identifies 'dormant code' for special analysis."

https://www.forcepoint.com/product/add-on/advanced-malware-detection

60. On information and belief, independent claim 19 is coextensive and representative of the scope of independent claim 10. Claim 19 is provided in an information storage media apparatus format that implements the method steps of claim 10. Accordingly, Plaintiff repeats and realleges paragraphs 40 - 47 as representative of the elements of claim 19.

61. On information and belief, independent claim 23 is coextensive and representative of the scope of independent claim 14. Claim 23 is provided in an information storage media apparatus format that implements the method steps of claim 14. Accordingly, Plaintiff repeats and realleges paragraphs 40 - 46 and 50 as representative of the elements of claim 14.

62. On information and belief, independent claim 24 is coextensive and representative of the scope of independent claim 15. Claim 24 is provided in an information storage media apparatus format that implements the method steps of claim 15. Accordingly, Plaintiff repeats and realleges paragraphs 40 - 46 and 53 as representative of the elements of claim 24.

63. On information and belief, independent claim 25 is coextensive and representative of the scope of independent claim 16. Claim 25 is provided in an information storage media apparatus format that implements the method steps of claim 16. Accordingly, Plaintiff repeats and realleges paragraphs 40 - 46 and 56 as representative of the elements of claim 25.

64. On information and belief, independent claim 27 is coextensive and representative of the scope of independent claim 18. Claim 27 is provided in an information storage media apparatus format that implements the method steps of claim 18. Accordingly, Plaintiff repeats and realleges paragraphs 40 - 46 and 59 as representative of the elements of claim 27.

65. On information and belief, Defendant's actions have and continue to constitute active inducing infringement of at least code inspection system claims 1-9, method claims 10-18, and information storage media claims 19-27 of the '698 patent in violation of 35 U.S.C. §271(b).

66. As a result of Defendant's infringement of at least code inspection system claims 1-9, method claims 10-18, and information storage media claims 19-27 of the '698 patent, Plaintiff Invicta has suffered monetary damages in an amount yet to be determined, and will continue to suffer damages in the future unless Defendant's infringing activities are enjoined by this Court.

Defendant is liable to Plaintiff in an amount that adequately compensates for such infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

67. Defendant's wrongful acts have damaged and will continue to damage Plaintiff Invicta irreparably, and Plaintiff has no adequate remedy at law for those wrongs and injuries. In addition to its actual damages, Plaintiff Invicta is entitled to a permanent injunction restraining and enjoining Defendant and its agents, servants, and employees, and all person acting thereunder, in concert with, or on its behalf, from infringing at least code inspection system claims 1-9, method claims 10-18, and information storage media claims 19-27 of the '698 patent.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Invicta respectfully requests that this Court enter:

A. A judgment in favor of Plaintiff Invicta that Defendant has been and is infringing at least claims 1-27 of the '698 patent pursuant to 35 U.S.C. §§ 271(a) and/or 271(b);

B. A permanent injunction enjoining Defendant and its officers, directors, agents, servants, affiliates, employees, divisions, branches, subsidiaries, parents, and all others acting in concert or privity with any of them from infringing, or inducing the infringement of, at least claims 1-27 of the '698 patent;

C. A judgment awarding Plaintiff Invicta all damages adequate to compensate it for Defendant's infringement of the '698 patent under 35 U.S.C. § 284, and in no event less than a reasonable royalty for Defendant's acts of infringement, including all pre-judgement and post-judgment interest at the maximum rate permitted by law, and also any past damages permitted under 35 U.S.C. § 286, as a result of Defendant's infringement of at least at least claims 1-27 of the '698 patent;

D. An assessment of costs, including reasonable attorney fees pursuant to 35 U.S.C. § 285, and prejudgment interest against Defendant; and

E. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Pursuant to FED. R. CIV. P. 38, Plaintiff Invicta hereby demands a trial by jury on all issues so triable.

Dated: March 5, 2020

Respectfully submitted,

By: /s/ Thomas M. Dunlap

Thomas M. Dunlap (Admitted W.D. Tex./VA
Bar No. 44016)
David Ludwig (Admitted W.D. Tex./VA Bar
No. 73157)
Dunlap Bennett & Ludwig PLLC
8300 Boone Blvd., Suite 550
Vienna, Virginia 22182
(703) 777-7319 (t)
(703) 777-3656 (f)
tdunlap@dbllawyers.com
dludwig@dbllawyers.com
ecf@dbllawyers.com

Attorneys for Invicta Networks, Inc.